(corresponding to US 2003/0126457 A1)

(9)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-198527
(43)Date of publication of application : 11.07.2003

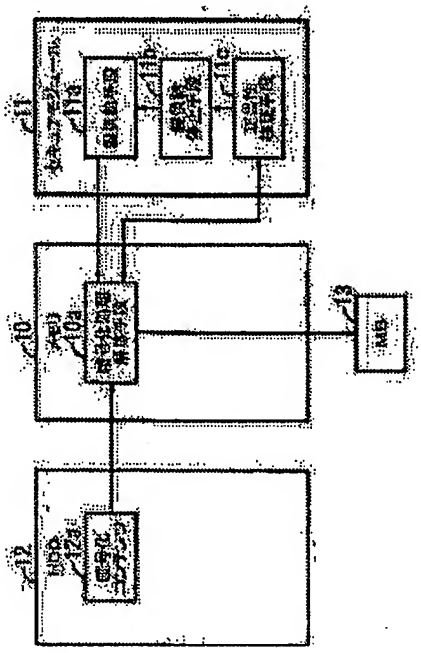
(51)Int.Cl. H04L 9/08
G06F 12/14
G06K 19/00
H04L 9/32

(21)Application number : 2001-397629
(22)Date of filing : 27.12.2001

(71)Applicant : FUJITSU LTD
(72)Inventor : KOBIYAMA KIYOYUKI
HASEBE TAKAYUKI

(54) INFORMATION REPRODUCING DEVICE AND SECURE MODULE

(57)Abstract:
PROBLEM TO BE SOLVED: To improve safety in an information reproducing device having an open architecture.
SOLUTION: A secure module 11 has a structure in which it is impossible to refer to internally stored information from the outside. a memory 10 has a structure in which reference from the outside is enabled. An enciphering processing cancel means 10a is packaged on the memory 10 and cancels enciphering processing applied to information by using a prescribed key. A key supply means 11a is packaged on the secure module 11 and supplies the key to the enciphering processing cancel means 10a. A correctness verifying means 11c is packaged on the secure module 11, supplies prescribed information to the enciphering processing cancel means 10a and verifies correctness of the enciphering processing cancel means 10a by referring to information answered as a result. A key supply stop means 11b is packaged on the secure module 11 and when correctness is not verified by the correctness verifying means 11c, the supply of the key by the key supply means 11a is stopped.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－198527
（P2003－198527A）
(43)公開日　平成15年７月11日(2003.7.11)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｂ０３５
Ｇ０６Ｋ　19/00		Ｇ０６Ｋ　19/00	Ｑ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｅ	
			６０１Ａ	

審査請求　未請求　請求項の数10　ＯＬ　（全 18 頁）

(21)出願番号　特願2001－397629(P2001－397629)

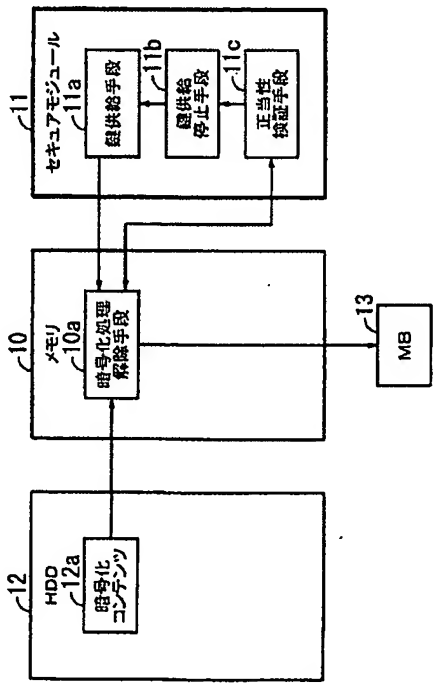
(22)出願日　平成13年12月27日(2001:12.27)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　小桧山　清之
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100092152
弁理士　服部　毅巌

最終頁に続く

(54)【発明の名称】　情報再生装置およびセキュアモジュール

(57)【要約】
【課題】　オープンアーキテクチャーを有する情報再生装置の安全性を高める。
【解決手段】　セキュアモジュール１１は、内部に格納されている情報を外部から参照することができない構造を有する。メモリ１０は、外部から参照することが可能な構造を有する。暗号化処理解除手段１０ａは、メモリ１０上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する。鍵供給手段１１ａは、セキュアモジュール１１上に実装され、暗号化処理解除手段１０ａに対して鍵を供給する。正当性検証手段１１ｃは、セキュアモジュール１１上に実装され、暗号化処理解除手段１０ａに対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段１０ａの正当性を検証する。鍵供給停止手段１１ｂは、セキュアモジュール１１上に実装され、正当性検証手段１１ｃによって正当性が認められない場合には、鍵供給手段１１ａによる鍵の供給を停止する。



1

【特許請求の範囲】

【請求項１】　伝送媒体によって伝送されてきた情報または記録媒体に格納されている情報を再生する情報再生装置において、

内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、

外部から参照することが可能なメモリと、

前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、

前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、

前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正当性を検証する正当性検証手段と、

前記セキュアモジュール上に実装され、前記正当性検証手段によって正当性が認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、

を有することを特徴とする情報再生装置。

【請求項２】　前記正当性検証手段は、前記暗号化処理解除手段に対して供給する前記所定の情報の初期値を、装置が起動されるたびに変更することを特徴とする請求項１記載の情報再生装置。

【請求項３】　前記正当性検証手段は、前記暗号化処理解除手段の正当性を検証するためのプロトコルを複数有しており、所定の周期で前記プロトコルを変更することを特徴とする請求項１記載の情報再生装置。

【請求項４】　前記鍵供給手段は、前記暗号化処理解除手段からの返答が所定の時間以上無い場合には、正当性が確認できないとして、前記鍵の供給を停止することを特徴とする請求項１記載の情報再生装置。

【請求項５】　前記メモリまたはセキュアモジュール上に実装されている複数の手段は、暗号化された状態で記録媒体に予め記録されており、必要に応じて暗号化が解除され、前記メモリまたはセキュアモジュール上に実装されることを特徴とする請求項１記載の情報再生装置。

【請求項６】　前記メモリ上に実装されている前記暗号化処理解除手段は、メモリ上に実装される度に、実現形態が異なることを特徴とする請求項１記載の情報再生装置。

【請求項７】　前記暗号化処理解除手段によって暗号化が解除された情報を外部に出力するための出力手段と、

前記暗号化処理解除手段によって暗号化が解除された情報を、前記出力手段に供給する際に、再度暗号化する暗号化手段と、

を更に有することを特徴とする請求項１記載の情報再生装置。

【請求項８】　前記暗号化手段は、複数の暗号化プロトコルから所定のプロトコルを選択して暗号化を行うことを特徴とする請求項７記載の情報再生装置。

2

【請求項９】　前記セキュアモジュールは着脱可能なデバイスによって構成されていることを特徴とする請求項１記載の情報再生装置。

【請求項１０】　伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールにおいて、

前記情報再生装置は、

外部から参照することが可能なメモリと、

前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、を有し、

前記セキュアモジュールは、

前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、

前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正当性を検証する正当性検証手段と、

前記セキュアモジュール上に実装され、前記正当性検証手段によって正当であると認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、

を有することを特徴とするセキュアモジュール。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は情報再生装置およびセキュアモジュールに関し、特に、伝送媒体によって伝送されてきた情報または記録媒体に格納されている情報を再生する情報再生装置および伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールに関する。

【０００２】

【従来の技術】近年、ブロードバンドインターネットやディジタル放送が普及しつつあり、配信されたコンテンツ（主にディジタルＡＶコンテンツ）の安全性を保障する権利保護技術がクローズアップされている。この中でも特にパーソナルコンピュータ（ＰＣ：Personal Computer）はオープンアーキテクチャーであり、基本的に誰でも覗き見ができるため、安全性の実現は困難とされている。

【０００３】しかし、一方でパーソナルコンピュータは、ブロードバンドインターネットの主要な出入り口であり、そこで安全性を保証できれば、インターネット全体でのディジタルＡＶコンテンツの配信が可能になり意義は大きい。

【０００４】従来は、パーソナルコンピュータのソフト上での権利保護は、安全性を保障するアルゴリズムの秘匿化、さらにアルゴリズムの解析を困難にする難読化が主流であった。しかしパーソナルコンピュータ上のソフトは、一旦、メインメモリ上に実装してしまえば、コピーすることは容易であり、コピーした結果を時間かけて解析することで、権利保護アルゴリズムを解析できる。非常に安全性に不安のある権利保護システムと考えられ、放送等公共性の高いシステムで一度解析されたことによる被害を考えると採用は困難である。

【０００５】図１０は、パーソナルコンピュータを用いた従来のシステムの構成例を示す図である。この図に示すように、従来のシステムは、パーソナルコンピュータ５０、ネットワーク５１、スピーカ５２、表示装置５３、および、入力装置５４によって構成されている。

【０００６】パーソナルコンピュータ５０は、ＣＰＵ（Central Processing Unit）５０ａ、ＲＯＭ（Read Only Memory）５０ｂ、ＲＡＭ（Random Access Memory）５０ｃ、ＨＤＤ（Hard Disk Drive）５０ｄ、ＭＢ（Multimedia Board）５０ｆ、Ｉ／Ｆ（Interface）５０ｇ，５０ｈ、および、バス５０ｉによって構成され、ネットワーク５１を介してダウンロードした情報を復号化してスピーカ５２および表示装置５３に出力する。

【０００７】ここで、ＣＰＵ５０ａは、ＨＤＤ５０ｄに格納されているプログラムに従って各種演算処理を実行するとともに、装置の各部を制御する。ＲＯＭ５０ｂは、ＣＰＵ５０ａが実行する基本的なプログラムやデータを格納している。

【０００８】ＲＡＭ５０ｃは、ＣＰＵ５０ａが各種演算処理を実行する際に、実行対象となるプログラムやデータを一時的に格納する。ＨＤＤ５０ｄは、ＣＰＵ５０ａが実行するプログラムやデータ等を格納している。

【０００９】ＭＢ５０ｆは、ＣＰＵ５０ａから供給された符号化された音声データや画像データを復号し、もとの音声信号や画像信号を生成して、スピーカ５２および表示装置５３に出力する。

【００１０】Ｉ／Ｆ５０ｇは、ネットワーク５１を介して情報を送受信する際のインターフェースであり、プロトコル変換やデータのフォーマット変換を実行する。Ｉ／Ｆ５０ｈは、入力装置５４から供給されたデータを、パーソナルコンピュータ５０の内部形式のデータに変換する。

【００１１】バス５０ｉは、ＣＰＵ５０ａ、ＲＯＭ５０ｂ、ＲＡＭ５０ｃ、ＨＤＤ５０ｄ、ＭＢ５０ｆ、および、Ｉ／Ｆ５０ｇ，５０ｈを相互に接続し、これらの間で情報の授受を可能にする。

【００１２】ネットワーク５１は、例えば、インターネットによって構成されており、ネットワーク上に接続されているサーバ等との間で情報を送受信する。スピーカ５２は、ＭＢ５０ｆから供給された音声信号を対応する音声に変換して出力する。

【００１３】表示装置５３は、例えば、ＣＲＴ（Cathode Ray Tube）モニターや液晶モニターによって構成されており、ＭＢ５０ｆから供給された画像信号を画像として表示する。

【００１４】入力装置５４は、例えば、マウスやキーボードによって構成されており、ユーザの操作に応じた情報を発生して出力する。図１１は、図１０に示すパーソナルコンピュータ５０における情報の流れを示す図である。

【００１５】この図に示すように、ＨＤＤ５０ｄには、基本ソフト、暗号解読鍵群、および、暗号化コンテンツが格納されている。ここで、基本ソフトは、暗号化コンテンツの暗号を解除するための処理等を行うためのソフトウエアであり、悪意あるユーザに解読されるのを防止するために、難読化されている。ここで、難読化とは、以下のような処理が施されていることをいう。

【００１６】難読化前　Ｘ＝Ｘ＋Ｙ
難読化後　Ｘ＝Ｘ＊２＋１＋Ｙ＊２－１
Ｘ＝Ｘ÷２
即ち、難読化前と後で演算結果は同じであるが、難読化後はアルゴリズムを解析するのが困難になっている。

【００１７】暗号解読鍵群は、暗号化コンテンツに施されている暗号を解読するための複数の鍵であり、悪意あるユーザに容易に取得されないようにするために、秘密のスクランブルが施され、また、秘密の場所に格納されている。

【００１８】暗号化コンテンツは、暗号化処理が施されたコンテンツであり、例えば、画像、音声、コンピュータデータ等から構成されている。暗号化コンテンツの再生が開始されると、以下の処理が実行される。

【００１９】（１）ＨＤＤ５０ｄから難読化されている基本ソフトが読み出され、ＲＡＭ５０ｃ上に実装される。

（２）その後、読み出された基本ソフトは、必要に応じて秘密の場所に格納され、秘密のスクランブルがかかった暗号解読鍵がＨＤＤ５０ｄから読み出される。暗号解読鍵は例えば、３～５箇所に分けて秘密の格納場所に格納され、更に、秘密の演算等を施さないと目的の鍵が得られないように処理されている。

【００２０】（３）暗号化コンテンツが読み出され、暗号解読鍵で暗号が解読される。

（４）続いて、暗号解読されたコンテンツが圧縮されている場合には、伸張処理（ビデオコンテンツの場合はＭＰＥＧ伸張処理、オーディオコンテンツの場合はＭＰＥＧオーディオ伸張処理など）が実行され、得られたデータがＲＡＭ５０ｃ上の画像バッファーおよび音声バッファーに格納された後、ＭＢ５０ｆに出力される。

【００２１】（５）ＭＢ５０ｆは、供給された音声データをＤ／Ａ変換処理するとともに、画像データに従って

描画処理を実行し、得られた音声信号をスピーカ５２へ出力し、一方、画像信号を表示装置５３に出力する。

【００２２】

【発明が解決しようとする課題】しかし、このような処理において、基本ソフトはパーソナルコンピュータ５０のＲＡＭ５０ｃに実装されるので、悪意のあるユーザによって解読されたり、コピーされたりする危険性を伴う。仮に、ＨＤＤ５０ｄに格納されている基本ソフトその他を全て暗号化したとしても、その暗号を解くためのソフトがパーソナルコンピュータ５０のどこかに存在すれば、そのソフトを解析して鍵の保存場所が特定されると、やはり基本ソフトは解析され権利保護アルゴリズムが判明してしまう。

【００２３】放送等、公共性の高い網では、アルゴリズムが判明しても容易にコンテンツの解読ができない処理法が望まれる。現行のハードウエア主体のデジタルテレビ受信機では、ＭＵＬＴＩ２、ＤＥＳ（Data Encryption Standard）などの暗号化が行われている。これらは、アルゴリズムは公知であるが、「暗号解読鍵」が判明しない限り、コンテンツの暗号を解読することは不可能である。

【００２４】しかし「暗号解読鍵」は、ハードウエアに内蔵され、ソフトウエア上には読み出すことはできないような構造となっている。更に、暗号解読回路やコンテンツ処理回路（ＭＰＥＧビデオ伸張やＭＰＥＧオーディオ伸張）もハードウエアで構成されているため、処理の内容を覗き見るのは極めて困難である。このため、ハードウエア主体のディジタル放送受信機は安全とされ、このようなシステムは実際に商用化が進んでいる。日本のパーフェクトＴＶ（商標）や米国のＤｉｒｅｃＴＶ（商標）などはこのような受信機の好例である。

【００２５】これに対しソフトウエア処理では、「暗号解読鍵」、「暗号解読回路」、「コンテンツ処理回路（ＭＰＥＧビデオ伸張やＭＰＥＧオーディオ伸張）」がソフトであり、こうした基本ソフト自体、さらには途中の演算結果も容易に読み取り可能なパーソナルコンピュータ５０上のＲＡＭ５０ｃに実装されるため、解析、覗き見が容易に行われてしまうという問題点があった。

【００２６】本発明はこのような状況に鑑みてなされたものであり、パーソナルコンピュータ等のオープンアーキテクチャーを有する装置に対して最低限のハードウエアを付加することで安全なソフトウエア処理を可能とする情報再生装置およびそのようなセキュアモジュールを提供することを目的とする。

【００２７】

【課題を解決するための手段】本発明では上記課題を解決するために、図１に示す、伝送媒体によって伝送されてきた情報または記録媒体（ＨＤＤ１２）に格納されている情報を再生する情報再生装置において、内部に格納されている情報を外部から参照することができない構造

を有するセキュアモジュール１１と、外部から参照することが可能なメモリ１０と、前記メモリ１０上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段１０ａと、前記セキュアモジュール１１上に実装され、前記暗号化処理解除手段１０ａに対して前記鍵を供給する鍵供給手段１１ａと、前記セキュアモジュール１１上に実装され、前記暗号化処理解除手段１０ａに対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段１０ａの正当性を検証する正当性検証手段１１ｃと、前記セキュアモジュール１１上に実装され、前記正当性検証手段１１ｃによって正当性が認められない場合には、前記鍵供給手段１１ａによる鍵の供給を停止する鍵供給停止手段１１ｂと、を有する情報再生装置が提供される。

【００２８】ここで、セキュアモジュール１１は、内部に格納されている情報を外部から参照することができない構造を有する。メモリ１０は、外部から参照することが可能な構造を有する。暗号化処理解除手段１０ａは、メモリ１０上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する。鍵供給手段１１ａは、セキュアモジュール１１上に実装され、暗号化処理解除手段１０ａに対して鍵を供給する。正当性検証手段１１ｃは、セキュアモジュール１１上に実装され、暗号化処理解除手段１０ａに対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段１０ａの正当性を検証する。鍵供給停止手段１１ｂは、セキュアモジュール１１上に実装され、正当性検証手段１１ｃによって正当性が認められない場合には、鍵供給手段１１ａによる鍵の供給を停止する。

【００２９】また、本発明では上記課題を解決するために、伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールにおいて、前記情報再生装置は、外部から参照することが可能なメモリと、前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、を有し、前記セキュアモジュールは、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正当性を検証する正当性検証手段と、前記セキュアモジュール上に実装され、正当性検証手段によって正当であると認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を有することを特徴とするセキュアモジュールが提供される。

【００３０】ここで、情報再生装置において、メモリ

は、外部から参照することが可能な構成を有する。暗号化処理解除手段は、メモリ上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する。一方、セキュアモジュールにおいて、鍵供給手段は、セキュアモジュール上に実装され、暗号化処理解除手段に対して鍵を供給する。正当性検証手段は、セキュアモジュール上に実装され、暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段の正当性を検証する。鍵供給停止手段は、セキュアモジュール上に実装され、正当性検証手段によって正当であると認められない場合には、鍵供給手段による鍵の供給を停止する。

【００３１】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は、本発明の動作原理を説明する原理図である。この図に示すように、本発明の情報再生装置は、メモリ１０、セキュアモジュール１１、ＨＤＤ１２、および、ＭＢ１３によって構成されている。

【００３２】ここで、メモリ１０は、例えば、ＲＡＭによって構成されており、ソフトウエアによって実現される暗号化処理解除手段１０ａが実装されている。セキュアモジュール１１は、例えば、ＰＣカードによって構成されている。このセキュアモジュール１１は、ＴＲＭ（Tamper Resistant Module）構造を有しているので、外部から覗き見を防止するとともに、内部のデータが改竄されることを防止することができる。

【００３３】なお、セキュアモジュール１１には、鍵供給手段１１ａ、鍵供給停止手段１１ｂ、正当性検証手段１１ｃが実装されている。ここで、鍵供給手段１１ａは、暗号化処理解除手段１０ａに対して暗号化を解除するための鍵を供給する。

【００３４】正当性検証手段１１ｃは、暗号化処理解除手段１０ａに対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段１０ａの正当性を検証する。

【００３５】正当性検証手段１１ｃによって暗号化処理解除手段１０ａが正当であると認められない場合には、鍵供給手段１１ａによる鍵の供給を停止する。ＭＢ１３は、メモリ１０上に実装されている暗号化処理解除手段１０ａによって暗号化が解除されたコンテンツを取得し、音声信号および画像信号に変換してスピーカおよび表示装置に供給する。

【００３６】次に、以上の原理図の動作について説明する。セキュアモジュール１１は、着脱可能なモジュールであり、例えば、鍵供給手段１１ａ、鍵供給停止手段１１ｂ、正当性検証手段１１ｃが実装された状態で、情報再生装置本体に装着することができる。

【００３７】メモリ１０に実装されている暗号化処理解除手段１０ａは、セキュアモジュール１１に予め格納しておき、これを起動時にメモリ１０に転写するか、あるいは、ＨＤＤ１２に暗号化した状態で格納しておき、起動時にメモリ１０に転写し、そこでセキュアモジュール１１に格納されている鍵を用いて暗号化処理を解除する。

【００３８】このような状態において、再生が開始されると、まず、正当性検証手段１１ｃは、暗号化処理解除手段１０ａに対して秘密の情報を供給する。暗号化処理解除手段１０ａは、秘密の情報を取得し、これに所定の処理を施すことにより、所定の情報を得る。そして、得られた情報を正当性検証手段１１ｃに供給する。

【００３９】正当性検証手段１１ｃは、暗号化処理解除手段１０ａから返答された情報を参照し、暗号化処理解除手段１０ａの正当性を検証する。その結果、暗号化処理解除手段１０ａが正当であると認められる場合は、鍵供給手段１１ａから暗号化処理解除手段１０ａに対して暗号化を解除するための鍵が供給される。

【００４０】一方、暗号化処理解除手段１０ａが正当であると認められない場合は、鍵供給停止手段１１ｂは、鍵供給手段１１ａから暗号化処理解除手段１０ａへの鍵の供給を停止させる。

【００４１】暗号化処理解除手段１０ａの正当性が確認された場合には、暗号化処理解除手段１０ａは、鍵供給手段１１ａから供給された鍵を用いて、ＨＤＤ１２から読み出した暗号化コンテンツ１２ａの暗号化を解除し、ＭＢ１３に供給する。

【００４２】ＭＢ１３は、暗号化処理解除手段１０ａから供給された、暗号化が解除されたコンテンツに含まれている音声データおよび画像データをそれぞれ音声信号および画像信号に変換し、図示せぬスピーカと、表示装置に供給する。

【００４３】再生処理が開始された後も、セキュアモジュール１１の正当性検証手段１１ｃは、暗号化処理解除手段１０ａに対して所定の周期で秘密の情報を供給し、その返答としての情報を検証することにより、暗号化処理解除手段１０ａが不正にコピーされたり改竄されたりすることを防止する。

【００４４】以上に示したように、本発明の情報再生装置では、外部から覗き見ることができないセキュアモジュール１１を設け、ここを起点としてメモリ１０に実装されている暗号化処理解除手段１０ａの正当性を検証し、正当性が確認できた場合には、鍵を供給するようにしたので、オープンアーキテクチャーを採用するパーソナルコンピュータ等においても、最小限のハードウエアを追加することにより、セキュリティを向上させることが可能になる。

【００４５】また、正当性検証手段１１ｃにより、暗号化処理解除手段１０ａの正当性を定期的に検証するようにしたので、メモリ１０に実装されている暗号化処理解除手段１０ａが不正に解析され、成りすまし等の改竄行為の発生を防止することが可能になる。

【００４６】次に、本発明の実施の形態について説明する。図２は、本発明の実施の形態の構成例を示す図である。この図に示すように、本発明の情報再生装置を含むシステムは、パーソナルコンピュータ（情報再生装置）５０、ネットワーク５１、スピーカ５２、表示装置５３、および、入力装置５４によって構成されている。

【００４７】パーソナルコンピュータ５０は、ＣＰＵ５０ａ、ＲＯＭ５０ｂ、ＲＡＭ５０ｃ、ＨＤＤ５０ｄ、セキュアモジュール５０ｅ、ＭＢ５０ｆ、Ｉ／Ｆ（Interface）５０ｇ，５０ｈ、および、バス５０ｉによって構成され、ネットワーク５１を介してダウンロードした情報を復号化してスピーカ５２および表示装置５３に出力する。

【００４８】ここで、ＣＰＵ５０ａは、ＨＤＤ５０ｄに格納されているプログラムに従って各種演算処理を実行するとともに、装置の各部を制御する。ＲＯＭ５０ｂは、ＣＰＵ５０ａが実行する基本的なプログラムやデータを格納している。

【００４９】ＲＡＭ５０ｃは、ＣＰＵ５０ａが各種演算処理を実行する際に、実行対象となるプログラムやデータを一時的に格納する。ＨＤＤ５０ｄは、ＣＰＵ５０ａが実行するプログラムやデータ等を格納している。

【００５０】セキュアモジュール５０ｅは、例えば、ＰＣ－ＣＡＲＤ等によって構成されており、ユーザの正当性を確認するための情報が格納されている。なお、セキュアモジュール５０ｅは、ＴＲＭ構造を有しているので、外部から覗き見を防止するとともに、内部のデータが改竄されることを防止することができる。

【００５１】ＭＢ５０ｆは、ＣＰＵ５０ａから供給された符号化された音声データや画像データを復号し、もとの音声信号や画像信号を生成して、スピーカ５２および表示装置５３に出力する。

【００５２】Ｉ／Ｆ５０ｇは、ネットワーク５１を介して情報を送受信する際のインターフェースであり、プロトコル変換やデータのフォーマット変換を実行する。Ｉ／Ｆ５０ｈは、入力装置５４から供給されたデータを、パーソナルコンピュータ５０の内部形式のデータに変換する。

【００５３】バス５０ｉは、ＣＰＵ５０ａ、ＲＯＭ５０ｂ、ＲＡＭ５０ｃ、ＨＤＤ５０ｄ、セキュアモジュール５０ｅ、ＭＢ５０ｆ、および、Ｉ／Ｆ５０ｇ，５０ｈを相互に接続し、これらの間でデータの授受を可能にする。

【００５４】ネットワーク５１は、例えば、インターネットによって構成されており、ネットワーク上に接続されているコンテンツサーバ等との間で情報を送受信する。スピーカ５２は、ＭＢ５０ｆから供給された音声信号を対応する音声に変換して出力する。

【００５５】表示装置５３は、例えば、ＣＲＴモニターや液晶モニターによって構成されており、ＭＢ５０ｆから供給された画像信号を画像として表示する。入力装置５４は、例えば、マウスやキーボードによって構成されており、ユーザの操作に応じた情報を発生して出力する。

【００５６】図３は、図２に示す実施の形態における情報の流れを示す図である。この図に示すように、ＨＤＤ５０ｄには、暗号化暗号解読鍵群、暗号化ソフト群、暗号化プロトコル群、および、暗号化コンテンツが格納されている。

【００５７】ここで、暗号化暗号解読鍵群は、暗号化コンテンツの暗号化を解除するための鍵の集合である。暗号化ソフト群は、暗号化を解除するための基本ソフトの集合である。

【００５８】暗号化プロトコル群は、暗号を解読する基本ソフトに対して挿入され、基本ソフトの正当性を検証するためのプロトコルの集合である。暗号化コンテンツは、暗号化されたコンテンツであり、例えば、暗号化された音声データや画像データによって構成されている。

【００５９】一方、セキュアモジュール５０ｅには、マスター鍵群、送信／返信受信ソフト、および、その他のソフトが存在する。ここで、マスター鍵群は、暗号化コンテンツを解読するための暗号化された鍵の集合である。

【００６０】送信／返信受信ソフトは、ＲＡＭ５０ｃ上に実装されている送信受信／返信ソフトとの間で情報を授受し、その正当性を検証する。また、その他のソフトは、例えば、プロトコルの初期値を変更するソフト、暗号化暗号の鍵を解読するための暗号化暗号鍵解読ソフト、任意の暗号化ソフト、任意の暗号化プロトコルを解読する任意暗号化プロトコル解読ソフト、任意のプロトコルを組み込むための任意プロトコル組み込みソフト、ソフトウエアをダウンロードするためのソフトウエアダウンロードソフト、暗号化コンテンツを解読するための暗号化コンテンツ解読ソフト、コンテンツを再度暗号化するためのコンテンツ再暗号化ソフト、コンテンツの暗号解読用の鍵を送信するためのコンテンツ暗号解読鍵送信ソフト、および、再暗号化されたコンテンツを送信するための再暗号化コンテンツ送信ソフトによって構成されている。

【００６１】ＲＡＭ５０ｃには、セキュアソフトが格納されており、このセキュアソフトには、基本ソフトが含まれる。基本ソフトには、送信受信／返信ソフト、メモリ領域変更ソフト、コンテンツ暗号解読鍵受信ソフト、再暗号化コンテンツ解読ソフト、コンテンツ処理ソフト、および、デコード画像コンテンツ出力ソフトが含まれている。

【００６２】ここで、送信受信／返信ソフトは、セキュアモジュール５０ｅからの送信を受信し、適当な応答を返す。メモリ領域変更ソフトは、セキュアモジュール５０ｅからの送信を受信し秘匿化必要データ（暗号解読

鍵、暗号解読後のＭＰＥＧビデオ／オーディオコンテンツ、ＭＰＥＧビデオ／オーディオ伸張後の情報格納領域など）が使用するメモリ領域を変更する。

【００６３】コンテンツ暗号解読鍵受信ソフトは、コンテンツの暗号を解読するための鍵を受信する。再暗号化コンテンツ解読ソフトは、セキュアモジュール５０ｅにおいて再暗号化されたコンテンツを解読するための鍵を受信する。

【００６４】コンテンツ処理ソフトは、ＭＰＥＧビデオ伸張ソフト、ＭＰＥＧオーディオ伸張ソフト等によって構成されている。デコード画像コンテンツ出力ソフトは、コンテンツ処理ソフトによって得られた画像コンテンツ等をＭＢ５０ｆに対して出力する。

【００６５】ＭＢ５０ｆでは、音声情報に対しては、Ｄ／Ａ変換処理等が施され、また、画像情報に対しては描画処理等が実行される。次に、本発明の実施の形態の動作の概要について以下に説明する。

【００６６】本実施の形態において、権利保護を行うための基本的な仕組みは以下の通りである。即ち、セキュアモジュール５０ｅから毎回セキュアソフトをＲＡＭ５０ｃにロードする。ロードしたセキュアソフトには、セキュアソフトの安全性を確認するための秘密の番号等を送信／受信するためにプロトコルが存在し、これがリアルタイムに通信することで安全性を確認する。

【００６７】その時、セキュアソフトをコピーされ、安全性確認用の秘密の番号などを解析されるのを防ぐため、以下の対策を実行する。

（１）セキュアモジュール５０ｅにタイマーを設け、送信／受信の間隔があまり長い場合はセキュアソフト改竄の可能性があるものとして、セキュアモジュール５０ｅからの暗号解読鍵提供の停止などの処置を講じる。

【００６８】（２）また、セキュアソフトをコピーされ、成りすまされるのを防止するため、同じ秘密の番号等が２度返信された場合等は、セキュアモジュール５０ｅからの暗号解読鍵提供の停止などの処置を講じる。

【００６９】（３）更に、毎回、例えば１時間程度の間隔で、セキュアソフト自体を置換する。このためにセキュアモジュール５０ｅ内、あるいは、ＨＤＤ５０ｄ内に複数（実際には無数）のセキュアソフトを準備し、その都度、異なるセキュアソフトをロードする。セキュアソフトの機能は同じであるが、安全性を確認するプロトコルや秘密の番号を毎回変更するようにする。このような構成により、例え、一度はセキュアソフトを解析されても、セキュアソフトの内容は毎回異なるので実質的に解析は不可能になる。基本的に１時間でセキュアソフトを解析し、演算結果等をファイル出力するように改竄するのは不可能と考えられるので、安全性は十分確保できる。

【００７０】なお、セキュアソフトの内容変更は、例えば送信、受信プロトコルのみを変更することで比較的簡単に行える。また、プロトコルの中の初期変数などを変えるだけでも変更を容易に実現することができる。

【００７１】例えば、以下のような秘密の番号を生成するプログラムを用いることにより、安全性確認用の送信、受信機能を実現できる。

Ｘ＝Ｘ＋Ｙ＊Ｚ＊Ｘ

ここで、Ｘは秘密の番号とし、ＹとＺは秘密の番号を生成するための初期変数である。Ｘ，Ｙ，Ｚの値を任意に変更するだけで無数の安全性確認プロトコルが生成できる。Ｘ＝１，Ｙ＝３，Ｚ＝５とすると、Ｘは、以下のように変化する。

【００７２】Ｘ＝１，１６，１６＋１６×１５，・・・もちろん、以上はほんの一例であり、このように簡単な方法では、初期値を変更してもＲＡＭ５０ｃが接続されているＰＣＩバスを介して内容を解析される可能性があるので、これ以外にも別の式を上の式に重畳させるのも良い。また、特別な一覧表によりＸがある値になったら強制的に他の値に変換する等の処理を行えば、基本式が漏洩した場合でも安全性は保てる。

【００７３】更に、ソフトを解析してこの式が判明しても、例えば、１時間毎にセキュアソフト自体を変更するようにすれば、解析が非常に困難になる。次に、以上の実施の形態の具体的な動作について説明する。このシステムの動作は以下の通りである。

【００７４】（１）所定のコンテンツを視聴しようとする場合には、ユーザは、電源を投入し、入力装置５４を操作して、表示装置５３に表示されている所定のアイコンをクリックする。

【００７５】（２）すると、セキュアモジュール５０ｅが起動し、ＨＤＤ５０ｄ内の複数の暗号化基本ソフトからランダムに一つを読み出す。

（３）次に、暗号化基本ソフトをセキュアモジュール５０ｅ内の暗号解読鍵と暗号解読ソフトで解読する。

【００７６】（４）次に、複数の暗号化プロトコルの中からランダムに適当なものを１つあるいは複数読み出し、セキュアモジュール５０ｅ内の暗号解読鍵と暗号解読ソフトで解読する。

【００７７】（５）暗号解読後の基本ソフトに暗号解読後の１つあるいは複数のプロトコルを挿入し、セキュアソフトを作成する。

（６）１つあるいは複数のプロトコルのそれぞれの初期値を初期化する。

【００７８】（７）初期化されたセキュアソフトをＲＡＭ５０ｃにロード（ダウンロード）し、セキュアソフトを起動する。セキュアモジュール５０ｅは、セキュアソフトがロードされ、起動されるとセキュアモジュール５０ｅ内のタイマーを参照して、あまり期間をおかずに（セキュアソフトの成りすましを防ぐため、時間をおかない）秘密の番号がセキュアソフトから、通信プロトコルに従って送信されるのを確認する。

【００７９】（８）セキュアモジュール５０ｅは、返しの秘密の番号を送信する。

（９）セキュアモジュール５０ｅは、更にまた秘密の番号が返信されるのを待つ。

【００８０】（１０）セキュアモジュール５０ｅは、内蔵されているタイマーを参照し、秘密の番号の返信に一定以上の時間がかかった場合は、セキュアソフトが改竄されたと見なし、セキュアソフトにエラー信号を渡して動作を停止させる。また、同一の秘密の番号が連続して返信された場合にも、セキュアソフトが改竄されたと見なし、セキュアソフトにエラー信号を渡して動作を停止させるようにしてもよい。

【００８１】（１１）一方、一定時間内に正常な返信があった場合には、セキュアモジュール５０ｅは、セキュアソフトの動作が正常とみなす。

（１２）セキュアモジュール５０ｅは、ＨＤＤ５０ｄから暗号化コンテンツを読み出し、暗号解読鍵を使って解読する。

【００８２】（１３）セキュアモジュール５０ｅは、暗号解読コンテンツを再暗号化する。

（１４）セキュアモジュール５０ｅは、再暗号化コンテンツをセキュアソフトに送信する。

【００８３】（１５）セキュアモジュール５０ｅは、更に、別のプロトコルでセキュアソフトの安全性をさらに確認後、再暗号化コンテンツ解読鍵をセキュアソフトに送信する。

【００８４】（１６）セキュアモジュール５０ｅは、コンテンツの再生が終了するか、または、終了の指示がユーザからなされるまで、上記（８）～（１６）の処理を繰り返す。

【００８５】一方、セキュアソフトは、以下の処理を実行する。

（１）セキュアソフトは、秘密の番号の送信受信を通してセキュアモジュール５０ｅから再暗号化コンテンツと再暗号化コンテンツ解読用の鍵を受信する。

【００８６】（２）セキュアソフトは、受信した再暗号化コンテンツ解読用の鍵を用いてコンテンツの解読を行う。

（３）セキュアソフトは、暗号解読の結果を、秘密の番号等の送信受信で決定された秘密のメモリ領域に対して、排他的論理和演算等の簡単なスクランブルを施した後に格納する。なお、格納先のメモリ領域は常時変更することにより、情報の漏洩を防止する。また、セキュアソフトが使用するレジスタについては、その都度変更するようにすれば、レジスタを媒介として内部の動作を解析されることを防止することができる。更に、秘密の番号を送受信する際には、割り込み禁止フラグをセットすることにより、他のソフトの割り込みを禁止し、割り込みによって内部の動作を解析されることを防止できる。なお、「秘密の番号の送受信」以外でも、解析を困難にする必要があるあらゆる箇所でこのように割り込み禁止フラグを活用することができる。

【００８７】（４）セキュアソフトは、格納された暗号解読されたコンテンツがＭＰＥＧ圧縮された画像データであるなら以下のようにＭＰＥＧビデオ伸張処理を施す。また、ＭＰＥＧ圧縮音声データであるならＭＰＥＧオーディオ伸張処理を施す。また、データ放送、字幕情報等他のコンテンツであるなら、それに応じた別の処理ルーチンに転送する。

【００８８】（５）セキュアソフトは、処理済みのコンテンツが、例えば、ＭＰＥＧ画像データである場合は、処理結果をＲＡＭ５０ｃ上のバッファー領域に格納する。なお、ＲＡＭ５０ｃ上の固定された領域に格納するようにすると、覗き見される可能性があるので、格納番地は、セキュアモジュール５０ｅとの交信によって設定される常時変化する番地に格納する。なお、格納番地を変更する以外にも、例えば、格納時にセキュアモジュール５０ｅとの交信によって設定される常時変化するスクランブル方法を採用することも可能である。

【００８９】（６）格納されたＭＰＥＧビデオデコード結果は、ＤＭＡ（Dynamic Memory Access）転送等でＭＢ５０ｆにＡＧＰバス等を介し転送され、ＭＢ５０ｆにおいてＡ／Ｄ変換処理を行い、モニター等で再生できる形式に変換されて表示される。なお、音声データの場合も基本的に同じような処理を経てスピーカに転送されて再生される。

【００９０】以上の実施の形態によれば、ＴＲＭ構成を有するセキュアモジュール５０ｅにより、ＲＡＭ５０ｃ上に実装されている基本ソフトの正当性を検証するようにしたので、オープンアーキテクチャーを有するシステムの安全性を高めることが可能になる。

【００９１】また、正当性を検証するためのプロトコルを所定の周期で変更するようにしたので、基本ソフトが覗き見された場合においても、安全性を確保することが可能になる。

【００９２】次に、本発明の第２の実施の形態について説明する。図４は、本発明の第２の実施の形態の構成例について説明する図である。この図に示すように、本発明の第２の実施の形態は、ＨＤＤ５０ｄに格納される情報を減少させ、その代わりにセキュアモジュール５０ｅのメモリ領域に権利保護情報を格納したことを特徴としている。

【００９３】この例では、ＨＤＤ５０ｄに格納されているのは、暗号化されたディジタルＡＶコンテンツ等のみである。一方、セキュアモジュール５０ｅには、（１）暗号化コンテンツを解読するための暗号化された鍵の集合であるマスター鍵群、（２）各プロトコル内秘密番号の計算式の初期値変更ソフト、（３）ソフト群、（４）プロトコル群、（５）任意プロトコルをセキュアソフトに組込むソフト、（６）ＲＡＭ５０ｃへ任意プロトコル

組込回路セキュアソフトをダウンロードするソフト、（７）セキュアソフトに送信／返信受信し、セキュアソフトの安全性を確認するためのソフト、（８）コンテンツ暗号解読鍵を送信するソフトが存在する。また、この他にも図示せぬタイマーを具備し、送信後の受信期間を測定し一定以上の期間が過ぎた場合はセキュアソフトへのコンテンツ暗号解読鍵の送信を停止する。

【００９４】ＲＡＭ５０ｃには、セキュアソフトが格納されており、このセキュアソフトには、基本ソフトが含まれる。基本ソフトには、以下のソフトが含まれている。即ち、基本ソフトには、（１）基本ソフトを受信するためのソフト、（２）送信受信／返信ソフト、（３）メモリ領域を変更するためのメモリ領域変更ソフト、（４）コンテンツ暗号解読鍵を受信するためのコンテンツ暗号解読鍵受信ソフト、（５）暗号化コンテンツを解読するための暗号化コンテンツ解読ソフト、（６）コンテンツ処理ソフト、（７）デコード画像コンテンツ出力ソフトが格納されている。

【００９５】また、セキュアモジュール５０ｅ、ＨＤＤ５０ｄ、ＲＡＭ５０ｃは、汎用のＰＣＩバスで相互に接続されて情報を交換し、ＲＡＭ５０ｃとＭＢ５０ｆはＡＧＰバス等のローカルバス（汎用バスと違い、傍受不可能）で接続される。

【００９６】次に、以上の実施の形態の動作について説明する。このシステムの動作は以下の通りである。

（１）ディジタル放送をＰＣ画面上で視聴したい場合、ユーザは、電源を投入した後、表示装置５３に表示されているディジタル放送受信用のアイコンをクリックする。

【００９７】（２）セキュアモジュール５０ｅが起動し、モジュール内の複数の基本ソフトからランダムに１つを読み出す。

（３）セキュアモジュール５０ｅは、次に、複数のプロトコルの中からランダムに適当なものを１つまたは複数読み出し、基本ソフトに１つまたは複数のプロトコルを挿入し、セキュアソフトを作成する。

【００９８】（４）セキュアモジュール５０ｅは、１つまたは複数のプロトコル上の初期値などを初期化する。

（５）セキュアモジュール５０ｅは、初期化されたセキュアソフトをＲＡＭ５０ｃにロード（ダウンロード）し、セキュアソフトを起動する。

【００９９】（６）セキュアモジュール５０ｅは、セキュアソフトがロードされ、起動されるとセキュアモジュール内のタイマーを参照し、所定の時間（セキュアソフトの成りすましを防ぐため短時間とする）が経過すると秘密の番号がセキュアソフトから、通信プロトコルに従って送信されるのを確認する。

【０１００】（７）セキュアモジュール５０ｅは、返しの秘密の番号を生成して送信する。

（８）セキュアモジュール５０ｅは、秘密の番号が返信されるのを待つ。

（９）セキュアモジュール５０ｅは、タイマーを参照し、秘密の番号の返信に一定以上の時間がかかる場合には、セキュアソフトが改竄された可能性があると見なし、セキュアソフトにエラー信号を渡して動作を停止させる。

【０１０１】（１１）一方、一定時間内に正常な返信が返った場合は、セキュアモジュール５０ｅは、セキュアソフトの動作が正常とみなし、更に、別のプロトコルでセキュアソフトの安全性を確認した後、暗号化コンテンツ解読鍵をセキュアソフトに送信する。

【０１０２】（１２）セキュアモジュール５０ｅは、この後は、上記（８）～（１２）の処理を繰り返す。一方、ＲＡＭ５０ｃ上のセキュアソフトは、以下の処理を実行する。

【０１０３】（１）セキュアモジュールとの秘密の番号の送信受信を通してＨＤＤ５０ｄから暗号化コンテンツを受信する。

（２）セキュアソフトは、セキュアモジュール５０ｅから暗号化コンテンツ解読用の鍵を受信する。

【０１０４】（３）セキュアソフトは、受信した鍵を用いて受信したコンテンツの暗号解読を行う。

（４）セキュアソフトは、暗号を解読した結果に対して、例えば、排他的論理和によるスクランブルを施した後、秘密の番号等の送受信によって決定された秘密のメモリ番地に格納する。なお、格納先のメモリ番地は、固定するのではなく、格納の度に変更するようにすることが望ましい。

【０１０５】（５）セキュアソフトは、暗号解読されたコンテンツは、もしそれがＭＰＥＧ圧縮された画像データなら以下のようにＭＰＥＧ画像伸張処理が施される。ＭＰＥＧ圧縮音声データならＭＰＥＧ音声伸張処理が施される。また、データ放送、字幕情報等他のコンテンツなら、それに応じた別の処理ルーチンに転送される。

【０１０６】（６）セキュアソフトは、処理されたコンテンツを、例えば、ＭＰＥＧ画像データの場合には、ＲＡＭ５０ｃのバッファー領域に転送する。なお、ＲＡＭ５０ｃの固定された番地に格納すると、覗き見される可能性があるので、格納番地は、セキュアモジュール５０ｅとの送受信の際に設定される番地（常に変化する番地）に格納される。なお、格納時にセキュアモジュールとの交信の中で設定される方法に基づいて、コンテンツをスクランブル処理するようにしてもよい。

【０１０７】（７）セキュアソフトは、格納されたＭＰＥＧ画像データを、ＤＭＡ転送等でＭＢ５０ｆにＡＧＰバス等を介し転送し、ＭＢ５０ｆによりＡ／Ｄ変換して、表示装置５３で再生可能な形式に変換する。

【０１０８】（９）セキュアソフトは、音声データについても、前述の画像データの場合と同様の処理により復号し、スピーカ５２に転送して再生する。以上に説明し

たように、本発明の第２の実施の形態では、マスター鍵等の情報についても、セキュアモジュール５０ｅに格納するようにしたので、ＨＤＤ５０ｄに格納する第１の実施の形態に比較して、セキュリティを更に向上させることが可能になる。

【０１０９】次に、本発明の第３の実施の形態について説明する。図５は、本発明の第３の実施の形態の構成例を示す図である。この図に示すように、本発明の第３の実施の形態では、図３に示す実施の形態と比較すると、ＲＡＭ５０ｃにスクランブル処理ソフトが追加されており、また、ＭＢ５０ｆにデスクランブル処理ソフトが追加されている。その他の構成は、図３の場合と同様であるので、その説明は省略する。

【０１１０】ここで、スクランブル処理ソフトは、ＭＰＥＧデコード処理等が施されたコンテンツに対して、所定のスクランブル処理を施す。一方、デスクランブル処理ソフトは、ＲＡＭ５０ｃにおいてスクランブル処理が施されたコンテンツに対してデスクランブル処理を施し、もとの情報を再生する。

【０１１１】次に、以上の実施の形態の動作について簡単に説明する。ＨＤＤ５０ｄおよびセキュアモジュール５０ｅでは、前述の場合と同様の処理により、鍵の送受信が行われた後、基本ソフトをＲＡＭ５０ｃ上にダウンロードしてそこに実装する。

【０１１２】ＲＡＭ５０ｃは、ダウンロードされた基本ソフトにより、セキュアモジュール５０ｅを介して暗号化コンテンツを受信し、暗号を解除する。そして、スクランブル処理ソフトは、暗号が解除されたコンテンツに対して所定のスクランブル処理を施し、ＭＢ５０ｆに対して送信する。

【０１１３】ＭＢ５０ｆは、ＲＡＭ５０ｃから送信されてきたスクランブルが施されたコンテンツを受信し、対応するデスクランブルソフトがデスクランブル処理を施し、もとのコンテンツデータを再生する。

【０１１４】そして、得られたコンテンツデータが音声信号である場合には、Ｄ／Ａ変換処理によりアナログ信号に変換してスピーカ５２に出力する。また、得られたコンテンツデータが画像データである場合には、描画処理により画像を描画した後、映像信号に変換し、表示装置５３に出力する。

【０１１５】以上のような実施の形態によれば、ＲＡＭ５０ｃからＭＢ５０ｆに供給されるコンテンツデータを不正に取り出すといった行為を防止することができる。

次に、本発明の第４の実施の形態について説明する。

【０１１６】図６は、本発明の第４の実施の形態の構成例を示す図である。この図に示す実施の形態では、図５に示す場合と比較して、セキュアモジュール５０ｅに通信プロトコル送信ソフトが追加され、また、ＭＢ５０ｆに通信プロトコル受信ソフトが追加されている。それ以外は、図５の場合と同様である。

【０１１７】ＲＡＭ５０ｃに格納されている通信プロトコル送信ソフトは、コンテンツデータに対するスクランブル方法や、コンテンツデータの出力順序を示す情報（通信プロトコル情報）をＭＢ５０ｆに対して送信する。

【０１１８】ＭＢ５０ｆに格納されている通信プロトコル受信ソフトは、通信プロトコル送信ソフトから送られてきた通信プロトコル情報を受信し、装置内部の該当する部分に供給する。

【０１１９】次に、以上の実施の形態の動作について簡単に説明する。コンテンツデータの再生が開始されると、セキュアモジュール５０ｅの通信プロトコル送信ソフトは、ＭＢ５０ｆに対して通信プロトコル情報を送信する。

【０１２０】通信プロトコル情報を受信したＭＢ５０ｆは、この情報に含まれているデスクランブル処理ソフトと、コンテンツの出力順序を示す情報とを抽出する。そして、抽出した情報に従ってコンテンツデータの順序を並べ替えするとともに、デスクランブル処理を施す。

【０１２１】ところで、通信プロトコル情報は、例えば、所定の時間間隔で送信され、送信の度にデスクランブル方法や出力順序が変更される。従って、悪意あるユーザによってＲＡＭ５０ｃ上に存在するスクランブル処理ソフトが解析された場合であっても、次のタイミングでは異なるスクランブル処理がなされていることから、不正使用を防止することが可能になる。

【０１２２】次に、本発明の第５の実施の形態の構成例について説明する。図７は、本発明の第５の実施の形態の構成例を示す図である。この図に示すように、本発明の第５の実施の形態は、ディジタル放送受信機の構成例である。

【０１２３】ここで、図７に示すディジタル放送受信機７０は、ディジタルチューナ７０ａ、ＭＵＬＴＩ２暗号解読部７０ｂ、Ｂ－ＣＡＳ（BS Conditional Access Systems）カード７０ｃ、ライセンス生成部７０ｄ、再暗号化処理部７０ｅ、ＨＤＤ７０ｆ、ＭＰＥＧデコーダ７０ｇ、暗号復号部７０ｈ、グラフィック処理部７０ｉ、再生ライセンス部７０ｊ、アナログ著作権保護部７０ｋ、および、ディジタル著作権保護部７０ｌによって構成されている。また、その外部には、パラボラアンテナ７１が接続されている。

【０１２４】ここで、ディジタルチューナ７０ａは、パラボラアンテナ７１によって捕捉された衛星からの電波を電気信号（ディジタル信号）に変換して出力する。ＭＵＬＴＩ２暗号解読部７０ｂは、ディジタルチューナ７０ａから出力されたディジタル信号に施されているＭＵＬＴＩ２暗号を解読し、もとのデータに復号して出力する。

【０１２５】Ｂ－ＣＡＳカード７０ｃは、ＩＣチップが内蔵されたプラスティック製のカードであり、ユーザの

正当性を保証するための情報が格納されている。ライセンス生成部７０ｄは、再暗号化に必要なライセンス情報を生成し、再暗号化処理部７０ｅに供給する。

【０１２６】再暗号化処理部７０ｅは、ＭＵＬＴＩ２暗号解読部７０ｂから供給されたディジタル信号を再度暗号化し、ＨＤＤ７０ｆに供給する。ＨＤＤ７０ｆは、再暗号化処理部７０ｅから供給されたデータを所定の領域に格納する。

【０１２７】暗号復号部７０ｈは、ＨＤＤ７０ｆから読み出されたデータに施されている暗号を復号し、もとのデータを生成する。ＭＰＥＧデコーダ７０ｇは、暗号復号部７０ｈから供給されたデータに対してＭＰＥＧデコード処理を施し、画像データおよび音声データを生成する。

【０１２８】グラフィック処理部７０ｉは、ＭＰＥＧデコーダ７０ｇから出力された画像データ等に基づいて描画処理を行い、もとの画像信号に変換して出力する。再生ライセンス部７０ｊは、暗号復号部７０ｈにおいて暗号を復号する際のライセンス情報を供給する。

【０１２９】アナログ著作権保護部７０ｋは、アナログ信号としての画像信号に対してコピー防止用の信号を重畳して出力する。ディジタル著作権保護部７０１は、ディジタル信号としての画像信号暗号化して出力する。

【０１３０】なお、この実施の形態においては、太線で示されている機能ブロック（ライセンス生成部７０ｄ、再暗号化処理部７０ｅ、および、再生ライセンス部７０ｊ）は、ＴＲＭによって構成され、内部の情報を参照することができない構造となっている。

【０１３１】また、機能ブロック間の結線であって、破線で示されている結線は、権利保護のために外部接続が禁止されている結線である。次に、以上の実施の形態の動作について説明する。

【０１３２】パラボラアンテナ７１によって捕捉された衛星からの電波は、ディジタルチューナ７０ａに供給され、そこで、ＭＰＥＧ－ＴＳディジタルストリームに変換されて出力される。

【０１３３】ＭＰＥＧ－ＴＳストリームには、複数の情報がＭＵＬＴＩ２暗号化された上で時分割多重化されており、ＭＵＬＴＩ２暗号解読部７０ｂは、Ｂ－ＣＡＳカード７０ｃから供給された暗号鍵等のライセンス情報を参照し、ＭＰＥＧ－ＴＳディジタルストリーム中の視聴者が選択した番組（特定ディジタルＡＶコンテンツ）を復号する。

【０１３４】再暗号化処理部７０ｅは、ライセンス生成部７０ｄから供給されるライセンス情報を参照し、ＡＶコンテンツを再暗号化し、ＨＤＤ７０ｆの所定の領域に格納する。

【０１３５】暗号復号部７０ｈは、ＨＤＤ７０ｆに格納された暗号化ディジタルＡＶコンテンツを再生する場合は、再生ライセンス部７０ｊから暗号を復号するための

ライセンス情報を取得し、暗号の復号処理を実行し、もとのＡＶコンテンツを生成する。

【０１３６】ＭＰＥＧデコーダ７０ｇは、暗号復号部７０ｈによって復号されたＡＶコンテンツに対してＭＰＥＧデコード処理を施しもとの画像データを再生し、グラフィック処理部７０ｉに供給する。

【０１３７】グラフィック処理部７０ｉは、ＭＰＥＧデコーダ７０ｇから供給された画像データに基づいて描画処理等のグラフィック処理を実行し、画像信号を生成する。そして、得られた画像信号をアナログ著作権保護部７０ｋとディジタル著作権保護部７０１に供給する。

【０１３８】アナログ著作権保護部７０ｋは、グラフィック処理部７０ｉから供給された画像信号の所定の部分に不正コピーを防止するための信号を重畳し、モニターに対して出力する。

【０１３９】ディジタル著作権保護部７０１は、グラフィック処理部７０ｉから供給された画像信号に対して暗号化処理を施し、モニターに対して出力する。ところで、以上の実施の形態においては、前述したように、太線で示す機能ブロック（ライセンス生成部７０ｄ、再暗号化処理部７０ｅ、および、再生ライセンス部７０ｊ）はＴＲＭ構造を有している。従って、図１に示すように、これらの機能ブロックに対して、鍵供給手段１１ａ、鍵供給停止手段１１ｂ、および、正当性検証手段１１ｃに該当する機能を設け、正当性を所定の時間間隔で検証するとともに、正当性が確認できない場合には、鍵の供給を停止するようにすれば、悪意のユーザによって受信したコンテンツが不正に使用されることを防止することができる。

【０１４０】次に、本発明の第６の実施の形態について説明する。図８は、本発明の第６の実施の形態の構成例を示す図である。この図に示すように、本発明の第６の実施の形態は、ディジタルチューナ８０ａ、ＭＵＬＴＩ２暗号解読部８０ｂ、Ｂ－ＣＡＳカード８０ｃ、再暗号化ライセンス生成部８０ｄ、ＨＤＤ８０ｅ、ソフト暗号復号再生ライセンス部８０ｆ、ソフトＭＰＥＧデコーダ８０ｇ、ソフトＡＡＣ（Advanced Audio Coding）デコーダ８０ｈ、グラフィック処理部８０ｉ、音声処理部８０ｊ、ＨＤＣＰ（High-bandwidth Digital Content Protection）ＬＳＩ８０ｋによって構成されている。また、その外部には、パラボラアンテナ８１が接続されている。

【０１４１】ここで、ディジタルチューナ８０ａは、パラボラアンテナ８１によって捕捉された衛星からの電波を電気信号（ディジタル信号）に変換して出力する。ＭＵＬＴＩ２暗号解読部８０ｂは、ディジタルチューナ８０ａから出力されたディジタル信号に施されているＭＵＬＴＩ２暗号を解読し、もとのデータに復号して出力する。

【０１４２】Ｂ－ＣＡＳカード８０ｃは、ＩＣチップが

内蔵されたプラスティック製のカードであり、ユーザの正当性を保証するための情報が格納されている。再暗号化ライセンス生成部８０ｄは、再暗号化に必要なライセンス情報を生成し、再暗号化処理を実行する。

【０１４３】ＨＤＤ８０ｅは、再暗号化ライセンス生成部８０ｄから供給されたデータを所定の領域に格納する。ソフト暗号復号再生ライセンス部８０ｆは、再生ライセンスを生成し、この再生ライセンスに従って、ＨＤＤ８０ｅから読み出されたデータに施されている暗号を復号し、もとのデータを生成する。

【０１４４】ソフトＭＰＥＧデコーダ８０ｇは、ソフト暗号復号再生ライセンス部８０ｆから供給されたＡＶコンテンツに対してＭＰＥＧデコード処理を施し、画像データを生成する。

【０１４５】ソフトＡＡＣデコーダ８０ｈは、音声信号を復号し、もとの音声データを生成して出力する。グラフィック処理部８０ｉは、ソフトＭＰＥＧデコーダ８０ｇから供給された画像データに対してグラフィック処理を施し、得られた画像信号をＨＤＣＰ　ＬＳＩ８０ｋに出力する。

【０１４６】ＨＤＣＰ　ＬＳＩ８０ｋは、グラフィック処理部８０ｉから供給された画像信号に対してＨＤＣＰ処理を施し、出力する。音声処理部８０ｊは、ソフトＡＡＣデコーダ８０ｈから出力される音声データをＤ／Ａ変換して出力する。

【０１４７】なお、以上の実施の形態において、太線で示されている機能ブロック（Ｂ－ＣＡＳカード８０ｃ、再暗号化ライセンス生成部８０ｄ、ソフト暗号復号再生ライセンス部８０ｆ）は、ＴＲＭによって構成され、内部の情報を参照することができない構造となっている。

【０１４８】また、ソフト暗号復号再生ライセンス部８０ｆ、ソフトＭＰＥＧデコーダ８０ｇ、および、ソフトＡＡＣデコーダ８０ｈは、ソフトウエアによって構成されている。

【０１４９】従って、ＴＲＭによって構成された部分を、図１に示すセキュアモジュール１１とし、ソフトウエアによって構成された部分を、図１に示すメモリ１０に対応付け、必要な機能を具備することにより、前述の場合と同様に悪意のユーザによって受信したコンテンツが不正に使用されることを防止することができる。

【０１５０】次に、本発明の第７の実施の形態について説明する。図９は、本発明の第７の実施の形態の構成例を示す図である。この図に示すように、本発明の第７の実施の形態は、ディジタルチューナ９０ａ、ＭＵＬＴＩ２暗号解読部９０ｂ、Ｂ－ＣＡＳカード９０ｃ、再暗号化ライセンス生成部９０ｄ、ＨＤＤ９０ｅ、ソフト暗号復号再生ライセンス部９０ｆ、ソフトＭＰＥＧデコーダ９０ｇ、ソフトＡＡＣデコーダ９０ｈ、グラフィック処理部９０ｉ、音声処理部９０ｊ、ＨＤＣＰ　ＬＳＩ９０ｋによって構成されている。また、その外部には、パラボラアンテナ９１が接続されている。なお、この実施の形態では、ＭＵＬＴＩ２暗号解読部９０ｂ、再暗号化ライセンス生成部９０ｄ、ソフト暗号復号再生ライセンス部９０ｆ、ソフトＭＰＥＧデコーダ９０ｇ、ソフトＡＡＣデコーダ９０ｈ、グラフィック処理部９０ｉ、および、音声処理部９０ｊは、ＬＳＩの内部に封入されている。

【０１５１】ここで、ディジタルチューナ９０ａは、パラボラアンテナ９１によって捕捉された衛星からの電波を対応する電気信号（ディジタル信号）に変換して出力する。

【０１５２】ＭＵＬＴＩ２暗号解読部９０ｂは、ディジタルチューナ９０ａから出力されたディジタル信号に施されているＭＵＬＴＩ２暗号を解読し、もとのデータに復号して出力する。

【０１５３】Ｂ－ＣＡＳカード９０ｃは、ＩＣチップが内蔵されたプラスティック製のカードであり、ユーザの正当性を保証するための情報が格納されている。再暗号化ライセンス生成部９０ｄは、再暗号化に必要なライセンス情報を生成し、再暗号化処理部を実行する。

【０１５４】ＨＤＤ９０ｅは、再暗号化ライセンス生成部９０ｄから供給されたデータを所定の領域に格納する。ソフト暗号復号再生ライセンス部９０ｆは、再生ライセンスを生成し、この再生ライセンスに従って、ＨＤＤ９０ｅから読み出されたデータに施されている暗号を復号し、もとのデータを生成する。

【０１５５】ソフトＭＰＥＧデコーダ９０ｇは、ソフト暗号復号再生ライセンス部９０ｆから供給されたＡＶコンテンツに対してＭＰＥＧデコード処理を施し、画像データを生成する。

【０１５６】ソフトＡＡＣデコーダ９０ｈは、音声信号を復号し、もとの音声データを生成して出力する。グラフィック処理部９０ｉは、ソフトＭＰＥＧデコーダ９０ｇから供給された画像データに対してグラフィック処理を施し、得られた画像信号をＨＤＣＰ　ＬＳＩ９０ｋに出力する。

【０１５７】ＨＤＣＰ　ＬＳＩ９０ｋは、グラフィック処理部９０ｉから供給された画像信号に対してＨＤＣＰ処理を施し、出力する。音声処理部９０ｊは、ソフトＡＡＣデコーダ９０ｈから出力される音声データをＤ／Ａ変換して出力する。

【０１５８】なお、以上の実施の形態において、ソフト暗号復号再生ライセンス部９０ｆ、ソフトＭＰＥＧデコーダ９０ｇ、および、ソフトＡＡＣデコーダ９０ｈは、ソフトウエアによって構成されている。

【０１５９】従って、ＬＳＩによって構成された部分を、図１に示すセキュアモジュール１１とし、ソフトウエアによって構成された部分を、図１に示すメモリ１０に対応付け、必要な機能を具備することにより、前述の場合と同様に悪意のユーザによって受信したコンテンツ

が不正に使用されることを防止することができる。

【０１６０】更に、本実施の形態では、ソフトウエアによって構成された部分もＬＳＩの内部に封入するようにしたので、更にセキュリティを向上させることが可能になる。

【０１６１】なお、以上の実施の形態に示すブロック図は、ほんの一例であり、本発明がこのような場合のみに限定されるものではないことはいうまでもない。また、以上の実施の形態において、ソフトウエアによって構成される部分は、適宜ハードウエアによって置換することが可能であることはいうまでもない。

【０１６２】（付記１） 伝送媒体によって伝送されてきた情報または記録媒体に格納されている情報を再生する情報再生装置において、内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、外部から参照することが可能なメモリと、前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正当性を検証する正当性検証手段と、前記セキュアモジュール上に実装され、前記正当性検証手段によって正当性が認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を有することを特徴とする情報再生装置。

【０１６３】（付記２） 前記正当性検証手段は、前記暗号化処理解除手段に対して供給する前記所定の情報の初期値を、装置が起動されるたびに変更することを特徴とする付記１記載の情報再生装置。

【０１６４】（付記３） 前記正当性検証手段は、前記暗号化処理解除手段の正当性を検証するためのプロトコルを複数有しており、所定の周期で前記プロトコルを変更することを特徴とする付記１記載の情報再生装置。

【０１６５】（付記４） 前記鍵供給手段は、前記暗号化処理解除手段からの返答が所定の時間以上無い場合には、正当性が確認できないとして、前記鍵の供給を停止することを特徴とする付記１記載の情報再生装置。

【０１６６】（付記５） 前記鍵供給手段は、前記暗号化処理解除手段から同一の返答が連続してなされた場合には、正当性が確認できないとして、前記鍵の供給を停止することを特徴とする付記１記載の情報再生装置。

【０１６７】（付記６） 前記メモリまたはセキュアモジュール上に実装されている複数の手段は、暗号化された状態で記録媒体に予め記録されており、必要に応じて暗号化が解除され、前記メモリまたはセキュアモジュール上に実装されることを特徴とする付記１記載の情報再生装置。

【０１６８】（付記７） 前記メモリ上に実装されている前記暗号化処理解除手段は、メモリ上に実装される度に、実現形態が異なることを特徴とする付記１記載の情報再生装置。

【０１６９】（付記８） 前記実現形態は、実装されるメモリ上の領域であることを特徴とする付記７記載の情報再生装置。

（付記９） 前記実現形態は、使用するメモリの領域であることを特徴とする付記７記載の情報再生装置。

【０１７０】（付記１０） 前記実現形態は、使用するレジスタの種類であることを特徴とする付記７記載の情報再生装置。

（付記１１） 前記暗号化処理解除手段によって暗号化が解除された情報を外部に出力するための出力手段と、前記暗号化処理解除手段によって暗号化が解除された情報を、前記出力手段に供給する際に、再度暗号化する暗号化手段と、を更に有することを特徴とする付記１記載の情報再生装置。

【０１７１】（付記１２） 前記暗号化手段は、複数の暗号化プロトコルから所定のプロトコルを選択して暗号化を行うことを特徴とする付記１１記載の情報再生装置。

（付記１３） 前記暗号化手段は、前記セキュアモジュールに格納されているプログラムを前記メモリ上に実装することにより実現されることを特徴とする付記１２記載の情報再生装置。

【０１７２】（付記１４） 前記メモリ上に実装される複数の手段は、その実行時に割り込み禁止フラグを立て、他のプログラムの割り込みが発生することを禁止することを特徴とする付記１記載の情報再生装置。

【０１７３】（付記１５） 前記セキュアモジュールに格納されているプログラムを、前記メモリ上に実装する際には、毎回異なる暗号化を施してメモリに供給することを特徴とする付記１記載の情報再生装置。

【０１７４】（付記１６） 前記セキュアモジュールは着脱可能なデバイスによって構成されていることを特徴とする付記１記載の情報再生装置。

（付記１７） 伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールにおいて、前記情報再生装置は、外部から参照することが可能なメモリと、前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、を有し、前記セキュアモジュールは、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正

当性を検証する正当性検証手段と、前記セキュアモジュール上に実装され、前記正当性検証手段によって正当であると認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を有することを特徴とするセキュアモジュール。

【０１７５】

【発明の効果】以上説明したように本発明では、伝送媒体によって伝送されてきた情報または記録媒体に格納されている情報を再生する情報再生装置において、内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、外部から参照することが可能なメモリと、メモリ上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、セキュアモジュール上に実装され、暗号化処理解除手段に対して鍵を供給する鍵供給手段と、セキュアモジュール上に実装され、暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段の正当性を検証する正当性検証手段と、セキュアモジュール上に実装され、正当性検証手段によって正当性が認められない場合には、鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を設けるようにしたので、オープンアーキテクチャー構成を有する、例えば、パーソナルコンピュータにより情報を再生する場合においても、最小限のハードウエアを追加することにより、安全なシステムを構築することができる。

【０１７６】また、本発明では、伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールにおいて、情報再生装置は、外部から参照することが可能なメモリと、メモリ上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、を有し、セキュアモジュールは、セキュアモジュール上に実装され、暗号化処理解除手段に対して鍵を供給する鍵供給手段と、セキュアモジュール上に実装され、暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段の正当性を検証する正当性検証手段と、セキュアモジュール上に実装され、正当性検証手段によって正当であると認められない場合には、鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を設けるようにしたので、情報再生装置に装着した場合に、最小限の構成でありながら、システムの安全性を高めることができるセキュリティーモジュールを提供することが可能になる。

【図面の簡単な説明】

【図１】本発明の動作原理を説明する原理図である。

【図２】本発明の実施の形態の構成例を示す図である。

【図３】図２に示す実施の形態における情報の流れを示す図である。

【図４】本発明の第２の実施の形態における情報の流れを示す図である。

【図５】本発明の第３の実施の形態における情報の流れを示す図である。

【図６】本発明の第４の実施の形態における情報の流れを示す図である。

【図７】本発明の第５の実施の形態の構成例を示す図である。

【図８】本発明の第６の実施の形態の構成例を示す図である。

【図９】本発明の第７の実施の形態の構成例を示す図である。

【図１０】パーソナルコンピュータを用いた従来のシステムの構成例を示す図である。

【図１１】図１０に示すパーソナルコンピュータにおける情報の流れを示す図である。

【符号の説明】

１０　メモリ
１０ａ　暗号化処理解除手段
１１　セキュアモジュール
１１ａ　鍵供給手段
１１ｂ　鍵供給停止手段
１１ｃ　正当性検証手段
１２　ＨＤＤ
１２ａ　暗号化コンテンツ
５０　パーソナルコンピュータ
５０ａ　ＣＰＵ
５０ｂ　ＲＯＭ
５０ｃ　ＲＡＭ
５０ｄ　ＨＤＤ
５０ｅ　セキュアモジュール
５０ｆ　ＭＢ
５０ｇ，５０ｈ　Ｉ／Ｆ
５０ｉ　バス
５１　ネットワーク
５２　スピーカ
５３　表示装置
５４　入力装置
７０　ディジタル放送受信機
７０ａ　ディジタルチューナ
７０ｂ　ＭＵＬＴＩ２暗号解読部
７０ｃ　Ｂ－ＣＡＳカード
７０ｄ　ライセンス生成部
７０ｅ　再暗号化処理部
７０ｆ　ＨＤＤ
７０ｇ　ＭＰＥＧデコーダ
７０ｈ　暗号復号部
７０ｉ　グラフィック処理部
７０ｊ　再生ライセンス部

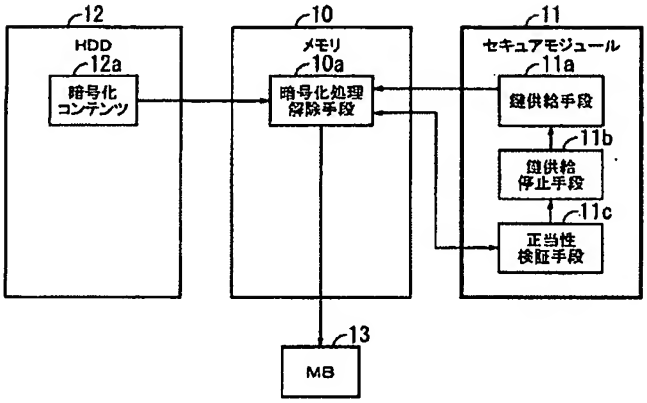
27

７０ｋ　アナログ著作権保護部
７０ｌ　ディジタル著作権保護部
７１　パラボラアンテナ
８０　ディジタル放送受信機
８０ａ　ディジタルチューナ
８０ｂ　ＭＵＬＴＩ２暗号解読部
８０ｃ　Ｂ－ＣＡＳカード
８０ｄ　再暗号化ライセンス生成部
８０ｅ　ＨＤＤ
８０ｆ　ソフト暗号復号再生ライセンス部
８０ｇ　ソフトＭＰＥＧデコーダ
８０ｈ　ソフトＡＡＣデコーダ
８０ｉ　グラフィック処理部
８０ｊ　音声処理部
８０ｋ　ＨＤＣＰ　ＬＳＩ

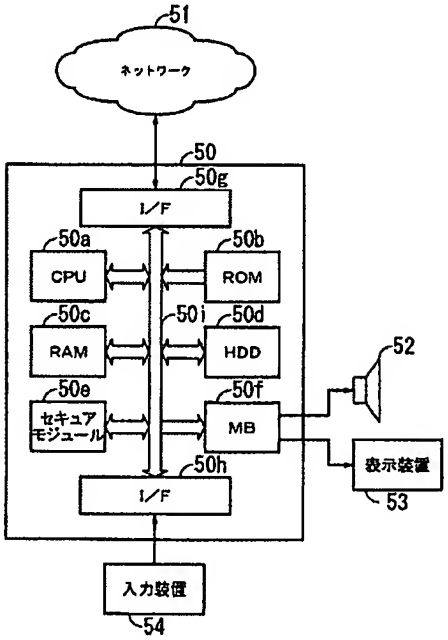
28

８１　パラボラアンテナ
９０　ディジタル放送受信機
９０ａ　ディジタルチューナ
９０ｂ　ＭＵＬＴＩ２暗号解読部
９０ｃ　Ｂ－ＣＡＳカード
９０ｄ　再暗号化ライセンス生成部
９０ｅ　ＨＤＤ
９０ｆ　ソフト暗号復号再生ライセンス部
９０ｇ　ソフトＭＰＥＧデコーダ
９０ｈ　ソフトＡＡＣデコーダ
９０ｉ　グラフィック処理部
９０ｊ　音声処理部
９０ｋ　ＨＤＣＰ　ＬＳＩ
９１　パラボラアンテナ

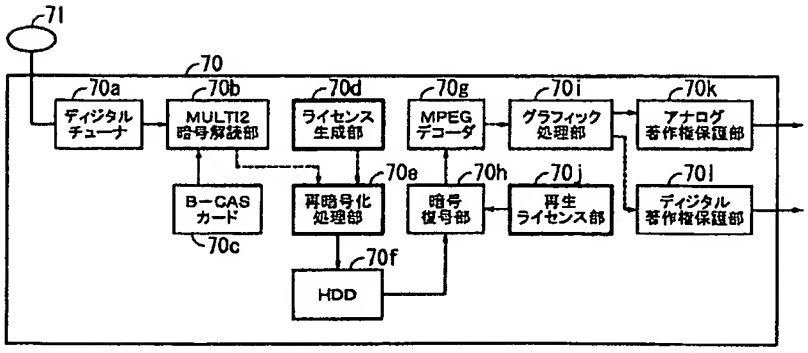
【図１】



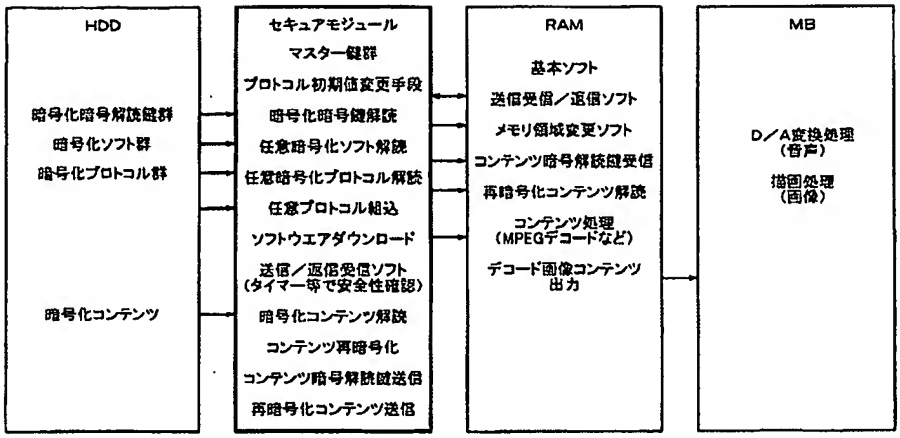
【図２】



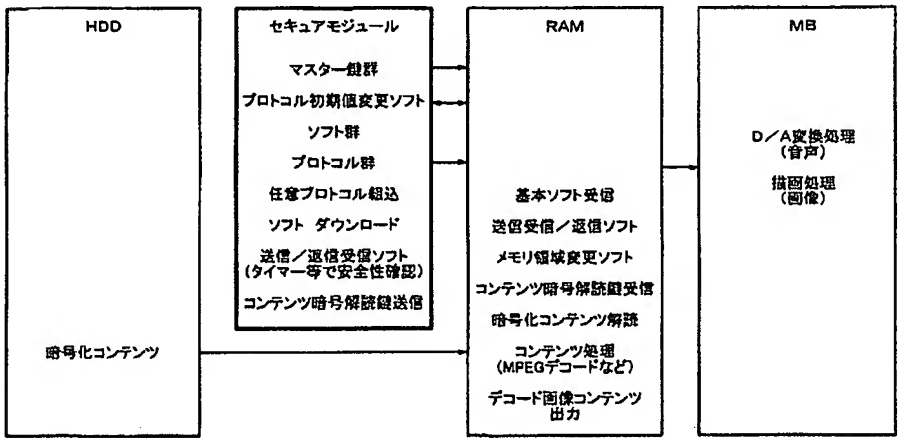
【図７】



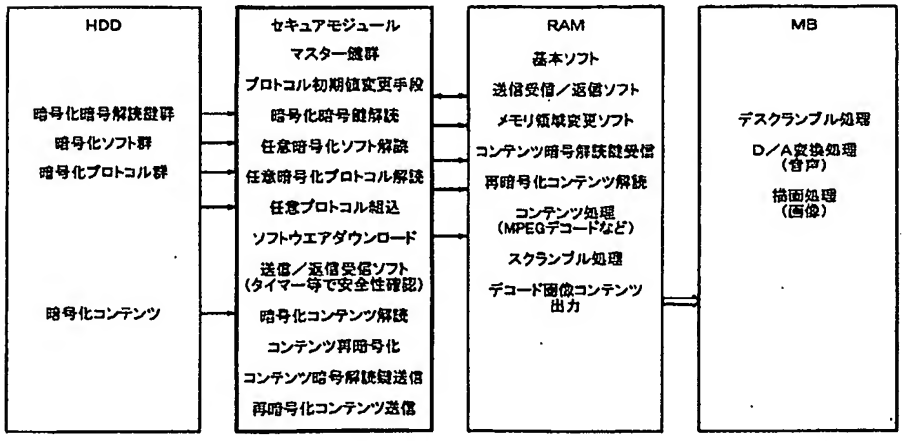
【図３】


HDD
暗号化暗号解読鍵群
暗号化ソフト群
暗号化プロトコル群
暗号化コンテンツ
セキュアモジュール
マスター鍵群
プロトコル初期値変更手段
暗号化暗号鍵解読
任意暗号化ソフト解読
任意暗号化プロトコル解読
任意プロトコル組込
ソフトウエアダウンロード
送信／返信受信ソフト
(タイマー等で安全性確認)
暗号化コンテンツ解読
コンテンツ再暗号化
コンテンツ暗号解読鍵送信
再暗号化コンテンツ送信
RAM
基本ソフト
送信受信／返信ソフト
メモリ領域変更ソフト
コンテンツ暗号解読鍵受信
再暗号化コンテンツ解読
コンテンツ処理
(MPEGデコードなど)
デコード画像コンテンツ
出力
MB
D／A変換処理
(音声)
描画処理
(画像)

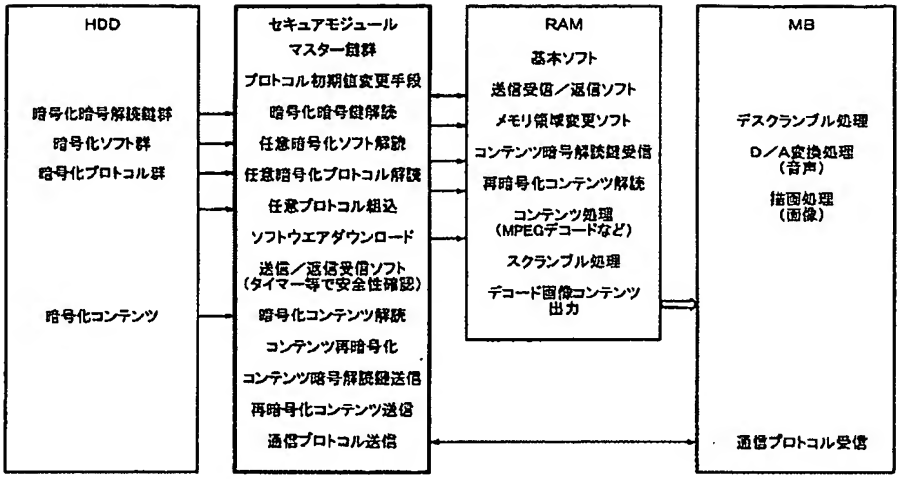
【図４】


HDD
暗号化コンテンツ
セキュアモジュール
マスター鍵群
プロトコル初期値変更ソフト
ソフト群
プロトコル群
任意プロトコル組込
ソフト ダウンロード
送信／返信受信ソフト
(タイマー等で安全性確認)
コンテンツ暗号解読鍵送信
RAM
基本ソフト受信
送信受信／返信ソフト
メモリ領域変更ソフト
コンテンツ暗号解読鍵受信
暗号化コンテンツ解読
コンテンツ処理
(MPEGデコードなど)
デコード画像コンテンツ
出力
MB
D／A変換処理
(音声)
描画処理
(画像)

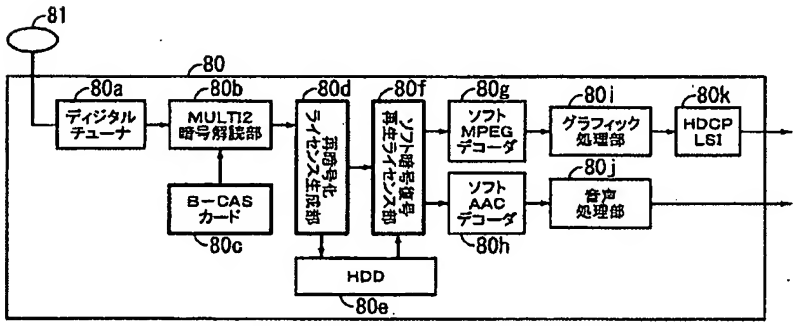
【図５】


HDD
暗号化暗号解読鍵群
暗号化ソフト群
暗号化プロトコル群
暗号化コンテンツ
セキュアモジュール
マスター鍵群
プロトコル初期値変更手段
暗号化暗号鍵解読
任意暗号化ソフト解読
任意暗号化プロトコル解読
任意プロトコル組込
ソフトウエアダウンロード
送信／返信受信ソフト
(タイマー等で安全性確認)
暗号化コンテンツ解読
コンテンツ再暗号化
コンテンツ暗号解読鍵送信
再暗号化コンテンツ送信
RAM
基本ソフト
送信受信／返信ソフト
メモリ領域変更ソフト
コンテンツ暗号解読鍵受信
再暗号化コンテンツ解読
コンテンツ処理
(MPEGデコードなど)
スクランブル処理
デコード画像コンテンツ
出力
MB
デスクランブル処理
D／A変換処理
(音声)
描画処理
(画像)

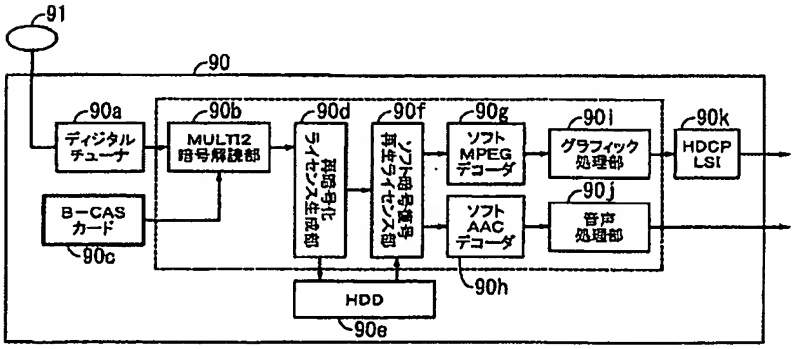
【図６】


HDD
暗号化暗号解読鍵群
暗号化ソフト群
暗号化プロトコル群
暗号化コンテンツ
セキュアモジュール
マスター鍵群
プロトコル初期値変更手段
暗号化暗号鍵解読
任意暗号化ソフト解読
任意暗号化プロトコル解読
任意プロトコル組込
ソフトウエアダウンロード
送信／返信受信ソフト
(タイマー等で安全性確認)
暗号化コンテンツ解読
コンテンツ再暗号化
コンテンツ暗号解読鍵送信
再暗号化コンテンツ送信
通信プロトコル送信
RAM
基本ソフト
送信受信／返信ソフト
メモリ領域変更ソフト
コンテンツ暗号解読鍵受信
再暗号化コンテンツ解読
コンテンツ処理
(MPEGデコードなど)
スクランブル処理
デコード画像コンテンツ
出力
MB
デスクランブル処理
D／A変換処理
(音声)
描画処理
(画像)
通信プロトコル受信

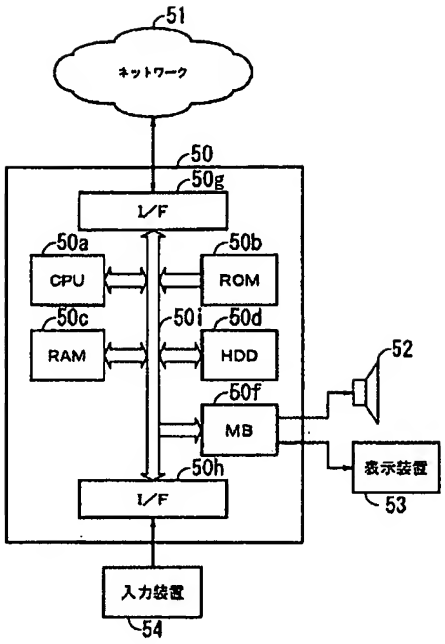
【図８】


81
80
80a
ディジタル
チューナ
80b
MULTI2
暗号解読部
80c
B－CAS
カード
80d
再暗号化
ライセンス生成部
80e
HDD
80f
ソフト暗号鍵等
再生ライセンス部
80g
ソフト
MPEG
デコーダ
80h
ソフト
AAC
デコーダ
80i
グラフィック
処理部
80j
音声
処理部
80k
HDCP
LSI

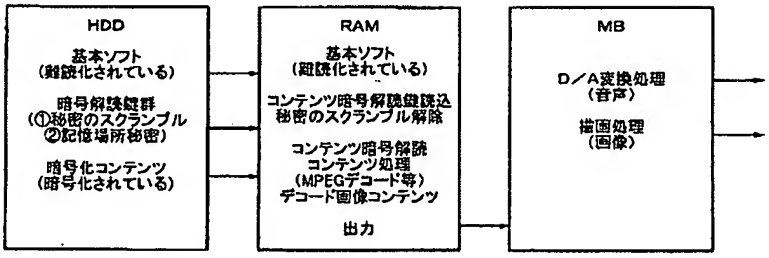
【図９】


91
90
90a
ディジタル
チューナ
90b
MULTI2
暗号解読部
90c
B－CAS
カード
90d
再暗号化
ライセンス生成部
90e
HDD
90f
ソフト暗号鍵等
再生ライセンス部
90g
ソフト
MPEG
デコーダ
90h
ソフト
AAC
デコーダ
90i
グラフィック
処理部
90j
音声
処理部
90k
HDCP
LSI

【図１０】



【図１１】



フロントページの続き

Ｆターム(参考) 5B017 AA03 BA07 BB03 CA07 CA16
5B035 AA13 BB09 CA11 CA29
5J104 AA16 AA34